UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/780,974	02/17/2004	Gary Kiwimagi	CN1-019US	1673

46317 7590 01/30/2007

TRENNER LAW FIRM, LLC
12081 WEST ALAMEDA PARKWAY #163
LAKEWOOD, CO 80228

EXAMINER	
AHUJA, SUPRIYA	
ART UNIT	PAPER NUMBER
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/780,974	KIWIMAGI ET AL.	
	Examiner	Art Unit	
	Supriya Ahuja	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02/17/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The abstract of the disclosure is objected to because on line 14, the phrase "then use" needs to be replaced by --then uses--. Correction is required. See MPEP § 608.01(b).

Claim Objections

2. **Claims 6, 8, 11, 12, 20** are objected to because of the following informalities:

In claim 6, line 2, the phrase "a secure authenticated connection" should be replaced with --another secure authenticated connection--.

In claim 8, line 5, the phrase "a data node" should be replaced with --the data node--.

In claim 11, line 5, the phrase "a secure authenticated connection" should be replaced with --another secure authenticated connection--.

In claim 12, line 12, the phrase "a secure authenticated connection" should be replaced with --another secure authenticated connection—and on line 10, the phrase "the data node" should be replaced by --the data node--.

In claim 20, lines 2 and 3, the phrase "the session database" should be replaced with --a session database-- and the phrase "the client session" should be replaced with --a client session--.

Appropriate correction is required.

Double Patenting

3. A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v.*

Eagle Mfg. Co., 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

4. **Claim 12** is rejected under 35 U.S.C. 101 as claiming the same invention as that of claim 11 of prior U.S. Co-pending Application No. 10/726,231. This is a double patenting rejection. Claim 11 of prior U.S. Co-pending Application No. 10/726,231 disclose all the limitation of claim 12 comprising a secure authenticated network connection between a client and a system node using a control node and a data node.

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

6. **Claims 1 and 8** are rejected under 35 U.S.C. 101 as claiming the same invention as that of claims 1 and 6 of U.S. Co-pending Application No. 10/726,231.

Claim 1 is rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Co-pending Application No. 10/726,231. Claim 1 discloses all limitations of claim 1 in the Co-pending Application No. 10/726,231 except for receiving at the data node a request from the client to access the system node and a request from the system node to access the client. The general concept of sending and receiving a request from the client and the server in order to communicate is well known in the art as an obvious communication technique. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify U.S. Co-pending Application No. 10/726,231 to send and receive requests in order to connect the client to the server.

Claim 8 is rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 6 of U.S. Co-pending Application No. 10/726,231. Claim 8 discloses all limitations of claim 6 in the Co-pending Application No. 10/726,231 except for receiving at the data node a request from the client to access the system node and a request from the system node to access the client. The general concept of sending and receiving a request from the client and the server in order to communicate is well known in the art as an obvious communication technique. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify U.S. Co-pending Application No. 10/726,231 to send and receive requests in order to connect the client to the server.

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. **Claims 8-11** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

In independent claim 8, a computer program product encoding computer programs for executing a computer process is being recited; however, it appears that the computer program product would reasonably be interpreted by one of ordinary skill in the art as software, per se, as evident on page 2 section [0023] of the specification. A computer program product can be considered authentication software as such claim 1 is classified as functional descriptive material. In addition, there is no evidence of the process being taking place on a computer in the claim. Therefore, dependent claims 9-11 are rejected under 35 U.S.C. 101 for the same and do not add any tangible result to the claim.

9. **Claims 12-18, 20** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

In independent claim 12, a system for establishing a secure authenticated network connection between a client and a system node is being recited; however, it appears that the system would reasonably be interpreted by one of ordinary skill in the art as software, per se. A system can be considered software as such claim 1 is classified as functional descriptive material. Therefore, dependent claims 13-18, 20 are rejected under 35 U.S.C. 101 for the same and do not add any tangible result to the claim.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. **Claims 1-20** are rejected under 35 U.S.C. 102(b) as being anticipated by Aoyama (US 4,995,112 dated 02/19/1991).

Claim 1. Aoyama discloses a method (security method, col. 2 line 8, Fig. 3) comprising: generating session information (access request data, col.1 lines 58 – 62; col. 2 lines 57-59) for a client (work station (WS), col.2 line 50), a system node (host units, col. 2 line 52-53), and a data node (directory, col. 2 line 66) if the client and system nodes satisfy at least one condition (security information, col. 2 line 59) for accessing each other; receiving at the data node a request from the client to access the system node and a request (access request, col. 1 lines 8-11; It is an established fact that a request is made in order to communicate from the client to the system and vice-versa through the data node) from the system node to access the client; and establishing a secure authenticated connection (col. 2 lines 15-20) between the client and the system node via the data node based at least in part on the session information.

Claim 2. Aoyama discloses the method with the step of (security method, col. 2 line 8, Fig. 3), receiving at a control node (pass through unit, col. 2 lines 60-64) a request (access request, col. 1 lines 8-11; It is an established fact that a request is made in order to communicate from the client

to the system and vice-versa through the data node) from the client (work station (WS), col.2 line 50) for the session information (access request data, col.1 lines 58 – 62; col. 2 lines 57-59).

Claim 3. Aoyama discloses the method with the step of (security method, col. 2 line 8, Fig. 3) registering (It is factual that in order to connect and get access to the server, the server's network address has to be registered, col. 3 lines 38-40) the system node (host units, col. 2 line 52-53) with a control node (pass through unit, col. 2 lines 60-64).

Claim 4. Aoyama discloses the method with the step of (security method, col. 2 line 8, Fig. 3), providing a list of (nodes 2,3, and 4, col. 2 line 53) registered system nodes (host units, col. 2 line 52-53) to the client (work station (WS), col.2 line 50), wherein the system node is selected at the client from the list of registered system nodes (col. 1 lines 15-23; where selection of the nodes from nodes 2, 3 and 4 is inherent in nature).

Claim 5. Aoyama discloses the method with the step of (security method, col. 2 line 8, Fig. 3), notifying the system node (host units, col. 2 line 52-53) when a message (access request, col. 1 lines 8-11; It is an established fact that a request is made in order to communicate from the client to the system and vice-versa through the data node) is received from the client (work station (WS), col.2 line 50) at the data node (directory, col. 2 line 66).

Claim 6. Aoyama discloses the method with the step of security method, col. 2 line 8, Fig. 3), establishing a secure authenticated connection (col. 2 lines 15-20) between the system node (host units, col. 2 line 52-53) and the data node (directory, col. 2 line 66).

Claim 7. Aoyama discloses the method with the step of (security method, col. 2 line 8, Fig. 3), sending the message (access request, col. 1 lines 8-11; It is an established fact that a request is made in order to communicate from the client to the system and vice-versa through the data

node) from the data node (directory, col. 2 line 66) to the system node (host units, col. 2 line 52-53) over the secure authenticated connection (col. 2 lines 15-20) between the system node and the data node.

Claim 8. Aoyama discloses a computer program product encoding computer programs (security method, col. 2 line 8, Fig. 3; it is inherent that the computer program product can be accomplished by a method) for executing on a control node (pass through unit, col. 2 lines 60-64) and a data node (directory, col. 2 line 66) a computer process, the computer process comprising: generating session information (access request data, col.1 lines 58 – 62; col. 2 lines 57-59) for a client (work station (WS), col.2 line 50), a system node (host units, col. 2 line 52-53), and a data node (directory, col. 2 line 66) if the client and system nodes satisfy at least one condition (security information, col. 2 line 59) for accessing each other; receiving at the data node a request from the client to access the system node and a request from the system node to access the client (access request, col. 1 lines 8-11; It is an established fact that a request is made in order to communicate from the client to the system and vice-versa through the data node); and establishing a secure authenticated connection (col. 2 lines 15-20) between the client and the system node via the data node based at least in part on the session information.

Claim 9. Aoyama discloses the computer program product wherein the computer process (security method, col. 2 line 8, Fig. 3; it is inherent that the computer program product can be accomplished by a method) at the control node (pass through unit, col. 2 lines 60-64) further comprises registering (It is factual that in order to connect and get access to the server, the server's network address has to be registered, col. 3 lines 38-40) the system node (host units, col. 2 line 52-53).

Claim 10. Aoyama discloses the computer program product wherein the computer process (security method, col. 2 line 8, Fig. 3; it is inherent that the computer program product can be accomplished by a method) at the control node (pass through unit, col. 2 lines 60-64) further comprises updating a client database (This is inherent that the client has a database of its own to store the address information and security information in a data structure, as any workstation does and therefore it is factual to update the database on a regular basis in order to access the network) with a dynamic network address (address information, col.1 lines 58 – 62) for the system node (host units, col. 2 line 52-53) on a recurring basis.

Claim 11. Aoyama discloses the computer program product wherein the computer process (security method, col. 2 line 8, Fig. 3; it is inherent that the computer program product can be accomplished by a method) at the data node (directory, col. 2 line 66) further comprises: notifying the system node (host units, col. 2 line 52-53) when a message (access request, col. 1 lines 8-11; It is an established fact that a request is made in order to communicate from the client to the system and vice-versa through the data node) is received from the client at the data node; establishing a secure authenticated connection (col. 2 lines 15-20) between the system node and the data node; and sending the message (access request, col. 1 lines 8-11; It is an established fact that a request is made in order to communicate from the client to the system and vice-versa through the data node) from the data node to the system node over the secure authenticated connection between the system node and the data node.

Claim 12. Aoyama discloses a system (security system, col. 1 lines 6-7) for establishing a secure authenticated network connection (col. 2 lines 15-20) between a client (work station (WS), col.2 line 50) and a system node (host units, col. 2 line 52-53), comprising: a control node

(pass through unit, col. 2 lines 60-64) linked to the client and the system node, the control node providing the client and the system node with session information (access request data, col.1 lines 58 – 62; col. 2 lines 57-59) if the client and system node satisfy at least one condition (security information, col. 2 line 59) for accessing each other; and a data node (directory, col. 2 line 66) communicatively coupled to the control node, the data node a request from the client to access the system node and a request from the system node to access the client (access request, col. 1 lines 8-11; It is an established fact that a request is made in order to communicate from the client to the system and vice-versa through the data node) and establishing a secure authenticated connection (col. 2 lines 15-20) between the client and the system node via the data node based at least in part on the session information.

Claim 13. Aoyama discloses the system (security system, col. 1 lines 6-7) wherein the session information (access request data, col.1 lines 58 – 62; col. 2 lines 57-59) includes at least a network address (address information, col.1 lines 58 – 62) for the system node (host units, col. 2 line 52-53).

Claim 14. Aoyama discloses the system (security system, col. 1 lines 6-7) wherein the session information (access request data, col.1 lines 58 – 62; col. 2 lines 57-59) includes at least a dynamic network address (address information, col.1 lines 58 – 62) for the system node (host units, col. 2 line 52-53).

Claim 15. Aoyama discloses the system (security system, col. 1 lines 6-7) wherein the session information (access request data, col.1 lines 58 – 62; col. 2 lines 57-59) includes a status (col. 1 lines 59-66) of the system node (host units, col. 2 line 52-53).

Claim 16. Aoyama discloses the system (security system, col. 1 lines 6-7) wherein the secure authenticated connection (col. 2 lines 15-20) between the data node (directory, col. 2 line 66) and the system node (host units, col. 2 line 52-53) is established in response to the data node receiving a message (access request, col. 1 lines 8-11; It is an established fact that a request is made in order to communicate from the client to the system and vice-versa through the data node) from the client (work station (WS), col.2 line 50).

Claim 17. Aoyama discloses the system (security system, col. 1 lines 6-7) further comprising a client database operatively associated with the control node (pass through unit, col. 2 lines 60-64), the client database (This is inherent that the client has a database of its own to store the address information and security information in a data structure, as any workstation does and therefore it is factual to update the database on a regular basis in order to access the network) including a data structure identifying system nodes (host units, col. 2 line 52-53) registered (It is factual that in order to connect and get access to the server, the server's network address has to be registered, col. 3 lines 38-40) with the control node.

Claim 18. Aoyama discloses the system (security system, col. 1 lines 6-7) wherein the data structure (This is inherent that the client has a database of its own to store the address information and security information in a data structure, as any workstation does and therefore it is factual to update the database on a regular basis in order to access the network) identifies authorized users (work station (WS), col.2 line 50) of the system nodes (host units, col. 2 line 52-53) registered (It is factual that in order to connect and get access to the server, the server's network address has to be registered, col. 3 lines 38-40) with the control node (pass through unit, col. 2 lines 60-64).

Claim 19. Aoyama discloses the system (security system, col. 1 lines 6-7) further comprising a session database (directory, col. 2 lines 65-68) operatively associated with the data node (external memory device, col. 2 lines 65-68, Fig. 4), the session database storing the session information (access request data, col.1 lines 58 – 62; col. 2 lines 57-59) received from the control node (pass through unit, col. 2 lines 60-64).

Claim 20. Aoyama discloses the system (security system, col. 1 lines 6-7) wherein the session information (access request data, col.1 lines 58 – 62; col. 2 lines 57-59) for a client session is removed from the session database when the client session ends (This is factual that the session information for a session is deleted on a regular basis or as soon as the session ends in the database in order to retain resources and space in the database).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Supriya Ahuja whose telephone number is 571-270-1588. The examiner can normally be reached on Monday - Thursday 7:30 -5:00; 2nd Friday 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Frantz Jules can be reached on 571-272-1808. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Supriya Ahuja

S.A.
January 22, 2007

FRANTZ JULES
SUPERVISORY PATENT EXAMINER